

Web Security - Hardening eStudy

Matthias Hecker, Andreas Schmidt, Philipp Promeuschel, Ivo
Senner, Andre Rein, Bartosz Boron, Christian Ketter, Christian
Thomas Weber

Fachhochschule Giessen-Friedberg

September 10th 2010



Links

■ Wiki-Dokumentation

- https://wiki.mni.fh-giessen-friedberg.de/index.php/WebSecurity_-_eStudy

■ Source-Code

- <https://trac.mni.fh-giessen.de/eStudy>



Inhalt

1 IPS System

- Thresholds
- Actions and commands
- IPS Configuration
- IPS at runtime
- IPS simulation mode

2 IPS Commands

3 Logs & Statistics

4 Version Check and Update

5 Suhosin

6 OWASP (Open Web Application Security Project)



Überblick

1 IPS System

- Thresholds
- Actions and commands
- IPS Configuration
- IPS at runtime
- IPS simulation mode

2 IPS Commands

3 Logs & Statistics

4 Version Check and Update

5 Suhosin

6 OWASP (Open Web Application Security Project)



IPS System

IPS Preview

- counteracts high impacts to secure the application
- is loaded when an impact is noticed from the IDS
- uses thresholds to evaluate impacts
- session based accumulation of small impact values
- executes different actions if thresholds are exceeded
- has 2 modes
 - simulation mode (log what would be done)
 - kick-ass mode



Thresholds

Thresholds

- thresholds can be configured for any tag from IDS
- possible to evaluate the type of attack and react different
- the thresholds are defined in the admin panel
- currently thresholds for 4 actions can be defined

Thresholds

Thresholds

IPS Thresholds (log, warn, kick, ban)	
SQL Injection	<input type="text" value="10, 40, 60, 80"/>
Cross site scripting	<input type="text" value="10, 40, 60, 80"/>
Remote code execution	<input type="text" value="10, 40, 60, 80"/>
Denial of service	<input type="text" value="10, 40, 60, 80"/>
Cross site request forgery	<input type="text" value="10, 40, 60, 80"/>
Information Disclosure	<input type="text" value="10, 40, 60, 80"/>
Local file inclusion	<input type="text" value="10, 40, 60, 80"/>
Remote file execution	<input type="text" value="10, 40, 60, 80"/>
Directory traversal	<input type="text" value="10, 40, 60, 80"/>



Actions and commands

Actions and commands

- Actions are: log, warn, kick and ban users
- an action is a list of commands which should be executed
- commands can be queued in these action lists and are executed in order of appearance
- Commands are:
 - logCommand
 - mailCommand
 - warnCommand
 - kickCommand (does also the ban)
- new commands can be inserted easily



IPS Configuration

IPS Configuration

IPS Einstellungen	
Aktiviert den Simulationsmodus des IPS	<input type="radio"/> Ja <input checked="" type="radio"/> Nein ?
Log-Datei für Simulationsmodus	<input type="text" value="/upload/phpids_ips_simulation.log"/> ?
Log-Datei für Log-Maßnahmen (log)	<input type="text" value="/upload/phpids_ips_impacts.log"/> ?
Dauer eines Zwangslogout (kick) in Sekunden	<input type="text" value="1800"/>



IPS at runtime

IPS at runtime

- load sessiondata or create them if new session
- accumulate the ids data to the session data
- check if any threshold is exceeded
- if so, initiate countermeasures



Simulation mode

Realization

- IPS is activated, but:
- Countermeasure are not performed
- Only logging of matching countermeasure

Useability

- IDS and IPS runnable in background (invisible for users)
- Admins can control IPS by simulation logs
- Adjustment of configs without worry



Simulation log file

```
-----
2010-09-10 13:33:00: Logging to './upload/phpids_ips_impacts.log', attacker: Anonymer Benutzer
2010-09-10 13:33:00: Warning attacker: Anonymer Benutzer
-----
2010-09-10 13:39:12: Logging to './upload/phpids_ips_impacts.log', attacker: Anonymer Benutzer
2010-09-10 13:39:12: Warning attacker: Anonymer Benutzer
-----
2010-09-10 13:39:47: Logging to './upload/phpids_ips_impacts.log', attacker: Anonymer Benutzer
2010-09-10 13:39:47: Warning attacker: Anonymer Benutzer
-----
2010-09-10 13:39:59: Logging to './upload/phpids_ips_impacts.log', attacker: Anonymer Benutzer
2010-09-10 13:39:59: Mailing to admins, kick of attacker: Anonymer Benutzer
2010-09-10 13:39:59: Kicking of attacker: Anonymer Benutzer
-----
2010-09-10 13:40:34: Logging to './upload/phpids_ips_impacts.log', attacker: Anonymer Benutzer
2010-09-10 13:40:34: Warning attacker: Anonymer Benutzer
-----
2010-09-10 13:40:54: Logging to './upload/phpids_ips_impacts.log', attacker: Anonymer Benutzer
2010-09-10 13:40:54: Mailing to admins, ban of attacker: Anonymer Benutzer
2010-09-10 13:40:54: Banning of attacker: Anonymer Benutzer
```



Configuring simulation mode

IPS Einstellungen

Aktiviert den Simulationsmodus des IPS

☒ Ja ☐ Nein



Log-Datei für Simulationsmodus



Log-Datei für Log-Maßnahmen (log)



Dauer eines Zwangslogout (kick) in Sekunden



Überblick

1 IPS System

- Thresholds
- Actions and commands
- IPS Configuration
- IPS at runtime
- IPS simulation mode

2 IPS Commands

3 Logs & Statistics

4 Version Check and Update

5 Suhosin

6 OWASP (Open Web Application Security Project)



Commands Overview:

- Log
- Warn
- Kick Ban
- Mail



Log

- All attacks, which above the warn-threshold, will be logged
- All logs will be saved in a file



Warn

- The attacker receives a warning
- The warning has no consequences for the attacker
- No admin will be informed
- It's displayed in the news-module



Kick&Ban

- The attacker will be logged out by force (session will be destroyed)
- All members of the admin-group will be informed by email and PM
- Kick: The account is inaccessible for half an hour (lock-time is adjustable)
- Ban: The account is inaccessible without time limitation. This implicates a necessary unban by an administrator.



Mail

The admin group will be notified by an email and a PM containing:

- Who is the attacker?
- When was the (possible) attack?
- How long will the attacker be blocked?
- Where can I get more information about the attacker and the attack?
- The link shows detail-information about the attack(s) from the user



What is adjustable?

- Which impact initiate which action (thresholds)
- The notification texts for the attacker (warn, kick, ban)
- Subject and message (with substitute symbols, e.g. *user*,time) of the notification-mails (kick, ban)



- - -



Überblick

1 IPS System

- Thresholds
- Actions and commands
- IPS Configuration
- IPS at runtime
- IPS simulation mode

2 IPS Commands

3 Logs & Statistics

4 Version Check and Update

5 Suhosin

6 OWASP (Open Web Application Security Project)



PHP-IDS Log

- phpids_intrusions table
- sort & filter options
- log emptying

Leere gesamten IDS-Log

Sortiere nach: Impact absteigend Los!

log green warn yellow kick orange

Intrusion Detection Logs						
Datum	Bezeichnung	Inhalt	Tags	Seite	Benutzer	Impact
2010-06-09 05:21:21	POST.coursename	f"><script>document.write(document.cookie)</script>	xss, csrf, id, rfe, ifi, sqli	/eS/courses/s_ettings.php	root 81.210.194.230 ip-81-210-194-230.un itymediagroup.de	40
2010-06-09 05:21:26	POST.coursename	f"><script>document.write(document.cookie)</script>	xss, csrf, id, rfe, ifi, sqli	/eS/courses/s_ettings.php	root 81.210.194.230 ip-81-210-194-230.un itymediagroup.de	40
2010-06-09 05:21:42	POST.coursename	f"><script>document.write(document.cookie)</script>	xss, csrf, id, rfe, ifi, sqli	/eS/courses/s_ettings.php	root 81.210.194.230 ip-81-210-194-230.un itymediagroup.de	40
2010-06-09 05:30:30	GET.Course	1-->>>"<sf100010v78048 2>	xss, csrf, id, sqli, ifi	/eS/veranst.php?Course=1-->>>"<sf100010v780482>	root 127.0.0.1 localhost	40
			xss, csrf, id, rfe, ifi, sqli		root	



PHP-IDS Statistics

- general table with key figures
- Sortierung: ALL | LAST 7 DAYS | LAST 24 HOURS

General Statistics					
ALL TIME		LAST 7 DAYS		LAST 24 HOURS	
Anzahl der Angriffe:	507	Anzahl der Angriffe:	4	Anzahl der Angriffe:	0
Durchschnittlicher Impact-Wert:	10.69	Durchschnittlicher Impact-Wert:	4.25	Durchschnittlicher Impact-Wert:	0
Höchster Impact-Wert:	52	Höchster Impact-Wert:	5	Höchster Impact-Wert:	
Angriffe pro Tag:	5.45	Angriffe pro Tag:	1.33	Angriffe pro Tag:	0
Anzahl Angreifer:	4	Anzahl Angreifer:	2	Anzahl Angreifer:	0
Anzahl schweren Angriffe:	32	Anzahl schweren Angriffe:	0	Anzahl schweren Angriffe:	0
Anzahl mittelschweren Angriffe:	97	Anzahl mittelschweren Angriffe:	0	Anzahl mittelschweren Angriffe:	0
Am meisten angegriffene Seite:	photogallery/newtopic.php	Am meisten angegriffene Seite:	announcement/create.php	Am meisten angegriffene Seite:	-

- statistics charts
- all data | user data

Impact-Wert:	Impact-Wert:	Impact-Wert:
Höchster Impact-Wert: 52	Höchster Impact-Wert: 5	Höchster Impact-Wert:
Angriffe pro Tag: 5.45	Angriffe pro Tag: 1.33	Angriffe pro Tag:
Anzahl Angreifer: 4	Anzahl Angreifer: 2	Anzahl Angreifer:
Anzahl schweren Angriffe: 32	Anzahl schweren Angriffe: 0	Anzahl schweren Angriffe:
Anzahl mittelschweren Angriffe: 97	Anzahl mittelschweren Angriffe: 0	Anzahl mittelschweren Angriffe:
Am meisten angegriffene Seite: photogallery/newtopic.php	Am meisten angegriffene Seite: announcement/create.php	Am meisten angegriffene Seite:

Diagramme:

Zeige Statistiken für: Bitte auswählen

Bitte auswählen

ALLGEMEINE STATISTIKEN

User

127.0.0.1

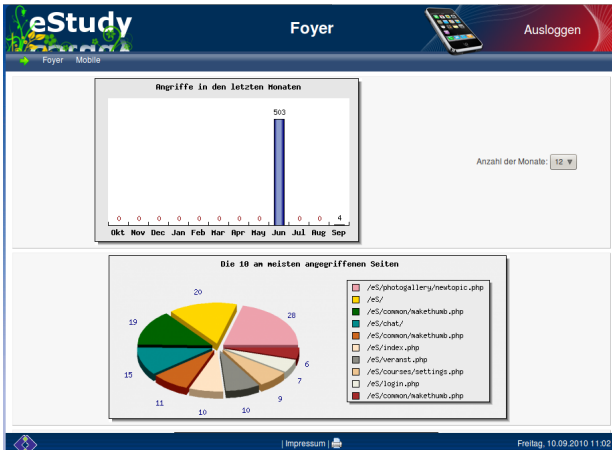
81.210.194.230

anonym

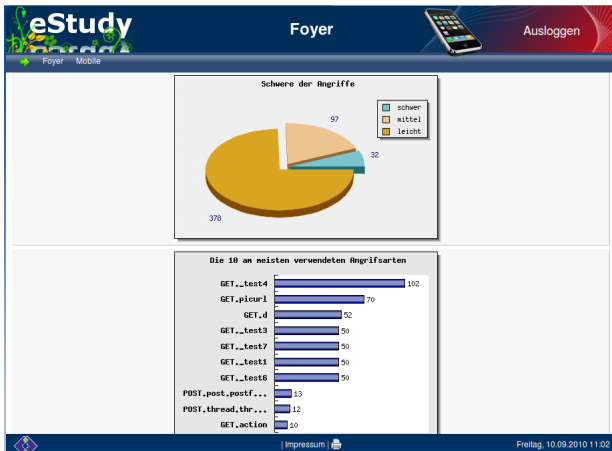
root



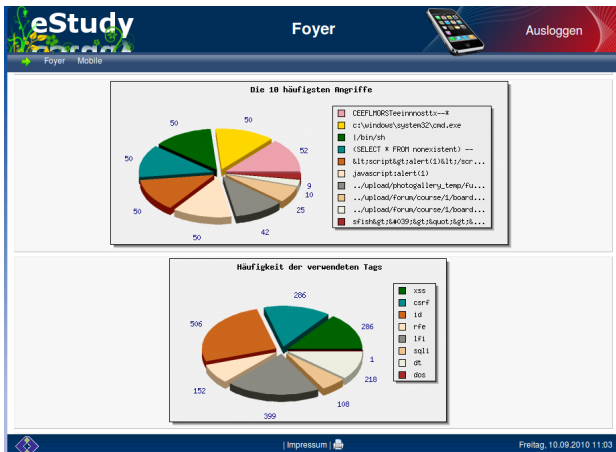
PHP-IDS Statistics



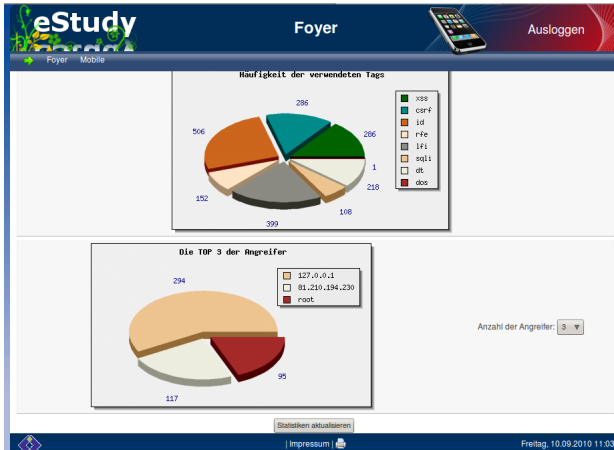
PHP-IDS Statistics



PHP-IDS Statistics



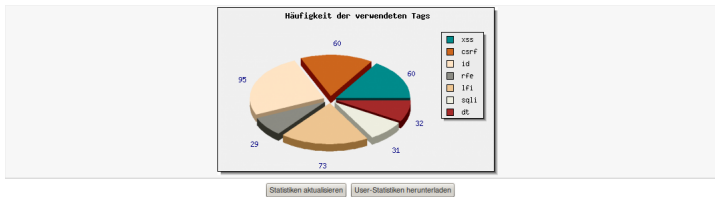
PHP-IDS Statistics



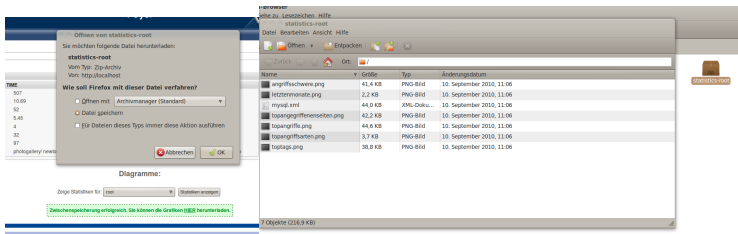


PHP-IDS Statistics

■ statistics download



PHP-IDS Statistics





PHP-IDS Statistics

```
-<mysql user="root">
-<row>
  <id>1</id>
  <name>POST.register_needed_information</name>
  <value>
    ShortName = Kurzname, string, -3 postcode = Postleitzahl, numeric, 15 location = Wohnort, string
  </value>
  <page>/eS/admin/settings.php</page>
  <tags>xss, csrf, id, rfe</tags>
  <ip>127.0.0.1</ip>
  <impact>4</impact>
  <origin>127.0.0.1</origin>
  <created>2010-09-07 03:28:40</created>
  <user_id>1</user_id>
</row>
-<row>
  <id>2</id>
  <name>POST.register_needed_information</name>
  <value>
    ShortName = Kurzname, string, -3 postcode = Postleitzahl, numeric, 15 location = Wohnort, string
  </value>
  <page>/eS/admin/settings.php</page>
  <tags>xss, csrf, id, rfe</tags>
  <ip>81.210.194.230</ip>
  <impact>4</impact>
  <origin>10.0.0.2</origin>
  <created>2010-06-09 03:47:33</created>
  <user_id>1</user_id>
</row>
-<row>
  <id>121</id>
  <name>POST.coursename</name>
  <value>
```




Überblick

1 IPS System

- Thresholds
- Actions and commands
- IPS Configuration
- IPS at runtime
- IPS simulation mode

2 IPS Commands

3 Logs & Statistics

4 Version Check and Update

5 Suhosin

6 OWASP (Open Web Application Security Project)



Version Check and Update

IDS Filter and Converter

- Retrieves Hashes and Modification Date from php-ids.org
- Version Check by Hash
- Validates File Integrity after Download
- Requires CURL PHP Module for HTTPS Downloads

IDS Version

Filter: **nicht aktuell.**
Letzte lokale Änderung: **10.09.2010 12:20**
Letzte Änderung auf php-ids.org: **09.08.2010 12:25**
SHA-1 Hash:
b9a147a93ade7540982ba792e54cc8a6a427a9d1(local)
099fae87b32b21739b7c91670ed785aae3e42108(remote)

Converter: **nicht aktuell.**
Letzte lokale Änderung: **10.09.2010 12:20**
Letzte Änderung auf php-ids.org: **11.08.2010 13:46**
SHA-1 Hash:
6d706892eb010c0d696730374d4f84b2f98e0c5c(local)
c45e84d7bd3c6c3f988874f834fdfb87da08ae37(remote)



Überblick

1 IPS System

- Thresholds
- Actions and commands
- IPS Configuration
- IPS at runtime
- IPS simulation mode

2 IPS Commands

3 Logs & Statistics

4 Version Check and Update

5 Suhosin

6 OWASP (Open Web Application Security Project)



Suhosin

- Custom configuration stored in .hataccess
- To ensure that the .htaccess-method works we have to set the perdir parameter in suhosin.ini/php.ini
- we added a custom logger script for Suhosin
- to run eStudy we had to whitelist the phar://- protocol
 - suhosin.executor.include.whitelist = "phar"
- HTTP Response Splitting, etc.



Suhosin Logger Script

- `suhosin.log.phpscript.name`
- The script is called with 2 variables registered in the current scope
 - `SUHOSIN_ERRORCLASS`
 - `SUHOSIN_ERROR`
- We parse `SUHOSIN_ERROR` and store the values into the Database

Suhosin Logger Script

- `suhosin_alerts` table
- version 0.1

Suhosin Logs				
<i>Alarm-Typ</i>	<i>Beschreibung</i>	<i>Betroffener Skript</i>	<i>Betroffene Zelle</i>	<i>IP des Angreifers</i>
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1
ALERT-SIMULATION	script tried to disable memory_limit by setting it to a negative value -1 bytes which is not allowed	/home/hks/NetBeansProjects/eStudy/trunk/web/suchmaschine/classes/class.spider.inc.php	43	127.0.0.1



ToDo

- There is still much to do to unleash the full power of Suhosin in combination with eStudy
- Especially these Suhosin-Settings need some work:
 - `suhosin.executor.func.blacklist`
 - `suhosin.executor.func.whitelist`



Überblick

1 IPS System

- Thresholds
- Actions and commands
- IPS Configuration
- IPS at runtime
- IPS simulation mode

2 IPS Commands

3 Logs & Statistics

4 Version Check and Update

5 Suhosin

6 OWASP (Open Web Application Security Project)



Top 10 WebSecurity Risks in eStudy



A1 - Injection/ A2 - Cross-Site Scripting (XSS)

- eStudy Data Class: Masking User Input
- IDS/IPS Protection:
- IDS detects attack vectors via pattern matching
- IPS prevents malicious requests / blocks users
- Suhosin fixes insecure php functions:
- HTTP Response Splitting, etc.



A3 - Broken Authentication and Session Management

- Suhosin limited protection:
 - Encryption of Session Cookies
 - Transparent protection against Session Hijacking
- Fixed Login Session Fixation



A4 - Insecure Direct Object References

- No global protection possible



A5 - Cross-Site Request Forgery (CSRF)

- eStudy built-in SecurityToken mechanism:
 - but not used everywhere



A6 - Security Misconfiguration

- phpsecinfo
- Suhosin limited protection:
 - enhances php security configuration
- new setup checks some settings



A7 - Insecure Cryptographic Storage

- Insecure eStudy User Passwords: MD5 hash without salt (default)
- Suhosin extensions:
 - `sha256` and `sha256_file` within php core



A8 - Failure to Restrict URL Access

- eStudy built-in security restrictions



A9 - Insufficient Transport Layer Protection

- eStudy supports automatic SSL (https) redirecting
- but: Cookies without secure flag



A10 - Unvalidated Redirects and Forwards

- No global protection possible